抽象代数

CHOUXIANG DAISHU

●李超 谢端强 冯良贵 编著●

国防科技大学出版社

抽 象 代 数

李 超 谢端强 冯良贵 编著

国防科技大学出版社
·长沙·

图书在版编目(CIP)数据

抽象代数/李超,谢端强,冯良贵编著.—长沙:国防科技大学出版社,2008.9
ISBN 978—7—81099—542—9

Ⅰ.抽… Ⅱ.①李…②谢…③冯… Ⅲ.抽象代数 Ⅳ.O153

中国版本图书馆 CIP 数据核字(2008)第 108010 号

国防科技大学出版社出版发行
电话:(0731)4572640 邮政编码:410073
http://www.gfkdcbs.com
责任编辑:石少平 责任校对:耿 筠
新华书店总店北京发行所经销
国防科技大学印刷厂印装
*
开本:850×1168 1/32 印张:6.75 字数:175 千
2008 年 9 月第 1 版第 1 次印刷 印数:1—1200 册
ISBN 978—7—81099—542—9
定价:16.00 元

前　言

代数学的发展与成熟是整个数学日趋完善的标志之一，代数学的方法已渗透到数学的各个分支。随着计算机的发展，代数结构的理论与方法已经成为解决信息科学和计算机科学中许多实际问题的有效工具。代数学是以代数结构作为研究对象的一门学科，古典代数学主要研究代数结构的元素特性，其中心问题是代数方程根的计算与分布，而抽象代数学从它产生的年代起就明显有别于古典代数学，它的主要研究对象不是代数结构中元素特性，而是各种代数结构本身特性以及不同代数结构之间的相互关系。掌握抽象代数学中所体现的丰富的数学思想与方法对于我们以后从事科学研究有着十分重要意义。

本教材根据我们1998年的抽象代数讲义改编付梓。本教材系统地介绍了抽象代数学的基本概念和基本知识，共六章。主要内容有：集合与映射、群的基本概念、群同态与群作用、Sylow 定理、环与环的同态、唯一分解整环、域扩张与有限域。

本教材力求做到：叙述深入浅出，文字生动活泼，推导自然流畅，例题充实新颖。

本教材与同类教材相比，其特色在于：(1)在群论中以较多的实例说明了群理论在平面对称图形分类、晶体学、分子结构理论和组合计数问题中的应用；(2)深入细致地介绍了域的扩张理论；(3)系统地介绍了有限域的代数结构特点，并引入了有限域在通信领

域中的两个应用实例。

本教材是集我们代数组全体同仁二十余年抽象代数课程的教学经验而成稿。由于编者水平有限，错误在所难免，不当之处欢迎各位专家指正。

编者

2008.7

目　录

第四章　环

第五章　域的扩张

第六章　有限域

第一章　集合与映射

集合与映射是数学中最基本的概念. 之所以称它们是最基本的，是因为这两个概念不能用其他的数学术语来严格定义，而只能给予形象的、直观的描述. 数学中把这样一些概念叫做原始概念，而其他的概念叫做派生概念. 本教材所介绍的群、环、域等代数结构都是由集合和映射而定义的派生概念.

§1.1　集合及其运算

具有确定的或适合一定条件的事物的全体，叫做**集合**. 组成集合的事物叫做集合的**元素**.

一般用 $A,B,C,\cdots$ 表示集合，而用 $a,b,c,\cdots$ 表示集合的元素. 如果没有特殊说明，$\mathbf{N}$、$\mathbf{Z}$、$\mathbf{Q}$、$\mathbf{R}$、$\mathbf{C}$ 分别表示自然数集、整数集、有理数集、实数集和复数集.

如果 a 是集合 A 中的元素，我们称 a **属于** A，记为 $a\in A$. 否则称 a **不属于** A，记为 $a\notin A$. 例如，$\sqrt{2}\in\mathbf{R}$，但 $\sqrt{2}\notin\mathbf{Q}$.

如果集合 A 中只含有有限个元素，我们称 A 为**有限集**. 否则称 A 为**无限集**. 当 A 为有限集时，我们用 $|A|$ 表示 A 中元素个数. 特别当 $|A|=0$，即 A 中不含任何元素时，我们称 A 为**空集**，

记为 $\varnothing$. 空集是一个特殊的集合.

集合的表示方法主要有下述四种：列举法、部分列举法、描述法(也称命题法)、归纳定义法.

列举法：将集合中全部元素一一列举出来，写在一对大括号内，用以表示集合，这种方法叫做列举法. 显然列举法只适用于表示元素不太多的有限集.

用 A 表示不超过 10 的自然数集合，则 A 可表示为

$$A = \{1,2,3,4,5,6,7,8,9,10\}.$$

部分列举法：将集合中一部分元素列举出来，其他元素用"…"来省略表示，所列举的元素能充分反映集合中全体元素的规律，这种方法叫做部分列举法.

仍用 A 表示不超过 10 的自然数集合，则 A 可表示为

$$A = \{1,2,3,\cdots,10\}.$$

同样，自然数集 N 和整数集 Z 也可用部分列举法表示为

$$\mathbf{N} = \{1,2,3,\cdots\},$$

$$\mathbf{Z} = \{\cdots,-2,-1,0,1,2,\cdots\} = \{0,\pm 1,\pm 2,\cdots\}.$$

描述法：为描述一个集合，首先给出一个命题，该命题具有下述性质：元素属于该集合的充分必要条件是元素满足该命题，这种表示集合的方法，我们称为描述法(又称命题法).

仍用 A 表示不超过 10 的自然数集合，则 A 可表示为

$$A = \{x \mid x \in \mathbf{N}, 1 \leqslant x \leqslant 10\}.$$

归纳定义法：首先已知集合中若干元素，并给出一组规则，由这些已知元素和给出的规则可产生集合中全部元素，这种表

示集合的方法叫做归纳定义法.

下面我们用归纳定义法表示集合 $A=\{1,2,3,\cdots,10\}$.

Step1：已知 $1\in A$；

Step2：如果 $n\in A$，并且 $n\leqslant 9$，则 $n+1\in A$.

由上述两步就可产生集合 A. 其中第一步称为归纳起点步，它主要明确集合中已知元素. 第二步称为归纳步，它主要给出一组规则，由此规则以及第一步中已知元素，便可产生集合中全部元素.

例 1.1　用不同的方法表示全体偶自然数集 E_v.

由于 E_v 为无限集，故 E_v 不能用列举法表示. 但它可以用部分列举法，描述法和归纳定义法描述.

部分列举法表示如下

$$E_v=\{2,4,6,8,10,\cdots\}.$$

描述法表示如下

$$E_v=\{n\mid n\in \mathbf{N},2\mid n\}.$$

归纳定义法表示如下

Step1：已知 $2\in E_v$；

Step2：如果 $n\in E_v$，则 $n+2\in E_v$.

由上述两步便可产生 E_v.

值得注意的是，并不是每个集合都象偶自然数集 E_v 一样，可用多种方法表示. 但一般而言，每个集合总可以用其中某一种方法表示.

下面我们来讨论集合的运算.

设 A,B 是两个集合，如果集合 A 中每个元素都是集合 B 中元素，我们称 A 是 B 的**子集**，记为 $A\subseteq B$. 如果 $A\subseteq B$ 且 $B\subseteq A$，则称 A 与 B **相等**，记为 $A=B$. 显然，每个集合是它自身的一个子集. 如果 A 是 B 的子集，并且 $A\neq B$，则称 A 为 B 的**真子集**，记为 $A\subset B$. 规定空集是任何集合的子集.

集合 A 的全体子集构成的集合，称为 A 的**幂集**，记为 2^A. 若 A 是有限集，则 2^A 也是有限集，且 $|2^A|=2^{|A|}$.

设 $A=\{1,2\}$，则 $2^A=\{\varnothing,\{1\},\{2\},\{1,2\}\}$. 以后我们称以集合作为元素的集合为**集族**. 幂集就是一个集族. 值得一提的是，空集 $\varnothing$ 和空集 $\varnothing$ 的幂集 $2^{\varnothing}=\{\varnothing\}$ 不是一回事. 前者不含任何元素，后者是以空集作为唯一元素的集合.

设 A,B 为任意两个集合，则 A 与 B 的**并集** $A\cup B$、**交集** $A\cap B$、**差集** $A-B$ 可用描述法定义如下

$$A\cup B=\{x\mid x\in A\text{ 或者 }x\in B\},$$

$$A\cap B=\{x\mid x\in A\text{ 并且 }x\in B\},$$

$$A-B=\{x\mid x\in A\text{ 并且 }x\notin B\}.$$

如果我们所考虑的集合都是某个大集合 X 的子集，我们称 X 为**全集**. 这时还可定义补集的概念，集合 A 在 X 中的**补集** A^c 定义为

$$A^c=\{x\mid x\in X,\text{但 }x\notin A\}.$$

上面我们定义了两个集合的并运算与交运算. 事实上，这两种运算可推广到任意多个集合.

设 D 为任意非空集，$\{A_\alpha\mid\alpha\in D\}$ 为集族，则

$$\bigcup_{\alpha\in D}A_\alpha=\{x\mid\text{存在}\alpha\in D,\text{使得}x\in A_\alpha\},$$

$$\bigcap_{\alpha\in D}A_\alpha=\{x\mid\text{对任意}\alpha\in D,\text{均有}x\in A_\alpha\}.$$

特别地，当 D 为自然数集 $\mathbf{N}$ 时，$\bigcup_{\alpha\in D}A_\alpha$ 和 $\bigcap_{\alpha\in D}A_\alpha$ 可分别记为 $\bigcup_{i=1}^{\infty}A_i$ 和 $\bigcap_{i=1}^{\infty}A_i$.

例 1.2　证明 $(-1,1)=\bigcup_{n=1}^{\infty}[-1+\frac{1}{n},1-\frac{1}{n}]$.

证明　对每个 $n\in\mathbf{N}$，

$$[-1+\frac{1}{n},1-\frac{1}{n}]\subseteq(-1,1),$$

从而由并集定义得

$$\bigcup_{n=1}^{\infty}[-1+\frac{1}{n},1-\frac{1}{n}]\subseteq(-1,1).$$

另一方面，对任意 $x_0\in(-1,1)$，则 $-1<x_0<1$. 又由于

$$\lim_{n\to\infty}(-1+\frac{1}{n})=-1,\qquad\lim_{n\to\infty}(1-\frac{1}{n})=1.$$

于是存在 $n_0\in\mathbf{N}$，使得 $-1+\frac{1}{n_0}<x_0<1-\frac{1}{n_0}$，从而

$$x_0\in[-1+\frac{1}{n_0},1-\frac{1}{n_0}]\subseteq\bigcup_{n=1}^{\infty}[-1+\frac{1}{n},1-\frac{1}{n}],$$

由 x_0 的任意性，

$$(-1,1)\subseteq\bigcup_{n=1}^{\infty}[-1+\frac{1}{n},1-\frac{1}{n}].$$

综合上面结果，

$$(-1,1)=\bigcup_{n=1}^{\infty}[-1+\frac{1}{n},1-\frac{1}{n}].$$　□

下面的定理 1.1 列出了集合运算的主要性质.

定理 1.1 设 A,B,C 为任意集合，$\{A_\alpha \mid \alpha \in D\}$ 是一个集族，则下列性质成立

(1) **幂等律** $A \cup A = A \cap A = A$；

(2) **交换律** $A \cup B = B \cup A, A \cap B = B \cap A$；

(3) **结合律** $(A \cup B) \cup C = A \cup (B \cup C)$，

$(A \cap B) \cap C = A \cap (B \cap C)$；

(4) **分配律** $(\bigcup_{\alpha \in D} A_\alpha) \cap A = \bigcup_{\alpha \in D} (A_\alpha \cap A)$，

$(\bigcap_{\alpha \in D} A_\alpha) \cup A = \bigcap_{\alpha \in D} (A_\alpha \cup A)$；

(5) **De Morgan 律** 设 X 为全集，$A_\alpha \subseteq X$，$\alpha \in D$，则

$$(\bigcup_{\alpha \in D} A_\alpha)^c = \bigcap_{\alpha \in D} A_\alpha^c,$$

$$(\bigcap_{\alpha \in D} A_\alpha)^c = \bigcup_{\alpha \in D} A_\alpha^c.$$

证明 我们只给出(5)的证明，其余性质由读者自证. 下面我们证明 $(\bigcup_{\alpha \in D} A_\alpha)^c = \bigcap_{\alpha \in D} A_\alpha^c$.

任取 $x \in (\bigcup_{\alpha \in D} A_\alpha)^c$，则 $x \notin \bigcup_{\alpha \in D} A_\alpha$，从而对每个 $\alpha \in D$，$x \notin A_\alpha$，即 $x \in A_\alpha^c$，于是由交集定义，$x \in \bigcap_{\alpha \in D} A_\alpha^c$，再由 x 的任意性，$(\bigcup_{\alpha \in D} A_\alpha)^c \subseteq \bigcap_{\alpha \in D} A_\alpha^c$.

另一方面，任取 $x \in \bigcap_{\alpha \in D} A_\alpha^c$，则对每个 $\alpha \in D$，均有 $x \in A_\alpha^c$，即对任意 $\alpha \in D$，$x \notin A_\alpha$，于是 $x \notin \bigcup_{\alpha \in D} A_\alpha$，也就是说 $x \in (\bigcup_{\alpha \in D} A_\alpha)^c$，再由 x 的任意性，$\bigcap_{\alpha \in D} A_\alpha^c \subseteq (\bigcup_{\alpha \in D} A_\alpha)^c$.

于是我们有

$$(\bigcup_{\alpha \in D} A_\alpha)^c = \bigcap_{\alpha \in D} A_\alpha^c.$$

类似地，可以证明性质(5)的第二个等式. □

§1.2 映射及其性质

设 A,B 为两个集合，如果存在一种对应规则 f，使得对 A 中每一个元素 x，在 B 中存在唯一的元素 y 与 x 对应，我们称 f 是从 A 到 B 的一个**映射**，记为 $f:A\to B$ 或 $y=f(x)$. 这时 y 称为 x 在 f 下的**象**，x 称为 y 在 f 下的一个**原象**.

例 1.3 设 $A=\{1,2,3\}$，$B=\{a,b,c\}$，令 $f(1)=a$，$f(2)=f(3)=b$，则 f 是从 A 到 B 的一个映射. 这个映射可用图 1.1 形象表示：

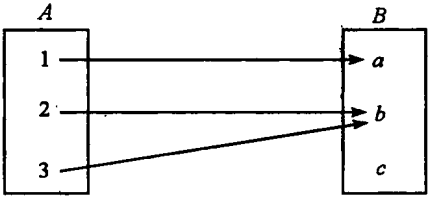

图 1.1

映射的一个最基本特点就是 A 中每一个元素有且只有一个象. 如果 A 中某个元素无象或者某个元素有多于一个象，则此对应规则就不是我们所讲的映射. 形象地说，映射的基本特征就是，A 中每一个点(元素)有且只有一条出边(例 1.3). 随着边的指向不同，我们得到不同的映射.

例 1.4 设 A 为 m 元集合，B 为 n 元集合，则从 A 到 B 的映射恰有 n^m 个.

证明 不妨设 $A=\{a_1,a_2,\cdots,a_m\}$，$B=\{b_1,b_2,\cdots,b_n\}$. 如果 f 是从 A 到 B 的映射，则对每个 $a_i(1\leqslant i\leqslant m)$ 而言，a_i 在 f 下的象 $f(a_i)$ 存在并且唯一. 随着 $(f(a_1),f(a_2),\cdots,f(a_m))$ 选取不同，则对应着不同的映射. 而每个 $f(a_i)$ 有 n 种选取方法(它可以取 B 中任何元素)，从而从 A 到 B 的映射共有 $\overbrace{n\cdot n\cdots n}^{m}=n^m$ 个. □

比如设 $A=\{1,2\}$，$B=\{a,b\}$，则从 A 到 B 的全部映射如图 1.2 所示.

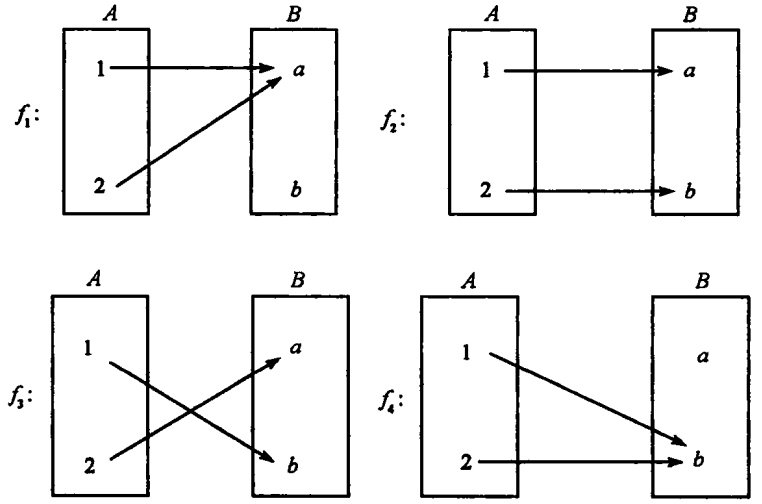

图 1.2

设 $f:A\to B$，$E\subseteq A$，$F\subseteq B$，令

$$f(E)=\{f(x)\mid x\in E\},$$

$$f^{-1}(F)=\{x\mid x\in A,f(x)\in F\},$$

则称 $f(E)$ 为 E 在 f 下的**象集**，$f^{-1}(F)$ 为 F 在 f 下的**原象集**.

定理 1.2　设 $f:A\to B,E\subseteq A,F\subseteq B$，则下列性质成立

(1) $E\subseteq f^{-1}(f(E))$；

(2) $f(f^{-1}(F))\subseteq F$；

(3) 设 $A_\alpha\subseteq A,B_\alpha\subseteq B$，这里 $\alpha\in D$，则

$$f(\bigcup_{\alpha\in D}A_\alpha)=\bigcup_{\alpha\in D}f(A_\alpha),$$

$$f(\bigcap_{\alpha\in D}A_\alpha)\subseteq\bigcap_{\alpha\in D}f(A_\alpha),$$

$$f^{-1}(\bigcup_{\alpha\in D}B_\alpha)=\bigcup_{\alpha\in D}f^{-1}(B_\alpha),$$

$$f^{-1}(\bigcap_{\alpha\in D}B_\alpha)=\bigcap_{\alpha\in D}f^{-1}(B_\alpha).$$

证明　(1) 对任意 $x\in E$，则 $f(x)\in f(E)$，于是 $x\in f^{-1}(f(E))$. 由 x 的任意性，$E\subseteq f^{-1}(f(E))$.

(2) 对任意 $y\in f(f^{-1}(F))$，则存在 $x\in f^{-1}(F)$，使得 $y=f(x)$，而 $f^{-1}(F)=\{x\mid x\in A,f(x)\in F\}$，故 $y=f(x)\in F$. 由 y 的任意性，$f(f^{-1}(F))\subseteq F$.

(3) 下面我们只证 $f(\bigcup_{\alpha\in D}A_\alpha)=\bigcup_{\alpha\in D}f(A_\alpha)$ 及 $f^{-1}(\bigcap_{\alpha\in D}B_\alpha)=\bigcap_{\alpha\in D}f^{-1}(B_\alpha)$，其余各款读者自证.

一方面，对任意 $y\in f(\bigcup_{\alpha\in D}A_\alpha)$，则存在 $x\in\bigcup_{\alpha\in D}A_\alpha$，使得 $y=f(x)$. 而由 $x\in\bigcup_{\alpha\in D}A_\alpha$ 可知，存在 $\alpha_0\in D$，使得 $x\in A_{\alpha_0}$，于是 $f(x)\in f(A_{\alpha_0})$，即 $y\in f(A_{\alpha_0})$，从而 $y\in\bigcup_{\alpha\in D}f(A_\alpha)$. 再由 y 的任意性，$f(\bigcup_{\alpha\in D}A_\alpha)\subseteq\bigcup_{\alpha\in D}f(A_\alpha)$.

另一方面，对任意 $y\in\bigcup_{\alpha\in D}f(A_\alpha)$，则存在 $\alpha_0\in D$，使得 $y\in$

$f(A_{\alpha_0})$，于是存在 $x \in A_{\alpha_0}$，使得 $y = f(x)$. 再由 $x \in A_{\alpha_0}$ 可得 $x \in \bigcup_{\alpha\in D} A_\alpha$，于是 $y = f(x) \in f(\bigcup_{\alpha\in D} A_\alpha)$. 由 y 的任意性，$\bigcup_{\alpha\in D} f(A_\alpha) \subseteq f(\bigcup_{\alpha\in D} A_\alpha)$. 从而我们有

$$\bigcup_{\alpha\in D} f(A_\alpha) = f(\bigcup_{\alpha\in D} A_\alpha).$$

再证 $f^{-1}(\bigcap_{\alpha\in D} B_\alpha) = \bigcap_{\alpha\in D} f^{-1}(B_\alpha)$.

任取 $x \in f^{-1}(\bigcap_{\alpha\in D} B_\alpha)$，于是 $f(x) \in \bigcap_{\alpha\in D} B_\alpha$，故对任意 $\alpha \in D$，$f(x) \in B_\alpha$，这表明 $x \in f^{-1}(B_\alpha)$. 由 α 的任意性，$x \in \bigcap_{\alpha\in D} f^{-1}(B_\alpha)$，于是

$$f^{-1}(\bigcap_{\alpha\in D} B_\alpha) \subseteq \bigcap_{\alpha\in D} f^{-1}(B_\alpha).$$

另一方面，对任意 $x \in \bigcap_{\alpha\in D} f^{-1}(B_\alpha)$，则对任意 $\alpha \in D$，$x \in f^{-1}(B_\alpha)$，于是 $f(x) \in B_\alpha$，由 α 的任意性知 $f(x) \in \bigcap_{\alpha\in D} B_\alpha$；故 $x \in f^{-1}(\bigcap_{\alpha\in D} B_\alpha)$. 由 x 的任意性，

$$\bigcap_{\alpha\in D} f^{-1}(B_\alpha) \subseteq f^{-1}(\bigcap_{\alpha\in D} B_\alpha).$$

从而我们有

$$f^{-1}(\bigcap_{\alpha\in D} B_\alpha) = \bigcap_{\alpha\in D} f^{-1}(B_\alpha). \qquad \square$$

例 1.5 考虑如图 1.3 所示映射.

令 $E = \{1,2\} \subseteq A$，$F = \{a,b,c\} \subseteq B$，$A_1 = \{1,2\}$，$A_2 = \{1,3\}$. 则直接计算可得

$$E \subset f^{-1}(f(E)) = A,$$

$$f(f^{-1}(F)) = \{a,b\} \subset F,$$

$$f(A_1 \cap A_2) \subset f(A_1) \cap f(A_2).$$

上例说明定理 1.2 中性质(1)，(2) 以及(3) 中第二条只是